UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/862,851	05/22/2001	Ralph S. Hoefelmeyer	COS 00 017	8371

25537 7590 11/21/2003

WORLDCOM, INC.
TECHNOLOGY LAW DEPARTMENT
1133 19TH STREET NW
WASHINGTON, DC 20036

EXAMINER	
ARANI, TAGHI T	

ART UNIT	PAPER NUMBER
2131	4

DATE MAILED: 11/21/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/862,851	HOEFELMEYER ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 May 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 3.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claims 1-30 were pending for examination.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 25-27 and 28-30 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 25 recites the limitation "the scanning computer systems" in line 17. There is insufficient antecedent basis for this limitation in the claim.

Dependent claims 26-27 are also rejected by virtue of their dependencies.

Claim 28 recites the limitation "the scanning computer systems" in line 16. There is insufficient antecedent basis for this limitation in the claim.

Claims 29-30 are also rejected by virtue of their dependencies.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 5 6-7, 9, 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over JI et al, US Pat. No. 5,623,600, issued April 1997 and further in view of Shanklin et al., US Pat. No. 6,578,147, filed Jan. 1999.

As per claims 1 and 9, JI is directed to a system for detecting and elimination viruses on a computer network which includes a File Transfer Protocol (FTP) proxy server, for controlling transfer of files and a Simple Mail Transfer Protocol (SMTP) proxy server for controlling the transfer of mail messages through the system, see abstract.

In a preferred embodiment, Ji discloses a gateway node (corresponding to a front-end) comprising a File Transfer protocol proxy server and a Simple Mail Transfer protocol proxy server for detecting (scanning) viruses (i.e. malicious code) in file transfers and messages and controlling data transfers to and from the gateway to and from a given network of which the gateway node is part, see col. 4, line 56 through col. 5, line 38, see also col. 10, line 26 through col. 11, line 40.

JI teaches that if a virus is detected, the proxy servers respond in variety of ways (i.e. countermeasures taken) according to user's needs specified in a configuration file, see col. 11, lines 3-40, and that an action is taken based on configuration settings, such as; 1) do nothing and transfer the mail message; 2) to transfer the mail message with the encoded portions that have been determined to have viruses; 3) rename the encoded portions of the message containing viruses, store the renamed portions as files in a specified directory on the proxy server and notify the user of the renamed files and directory path which can be used to manually request the file from the system administrator ; 4) writing the output of virus-checking program into the mail message in place of encoded portions and sending the mail message. The teaching of JI clearly

suggests a detection management system employed on the gateway connected to the proxy servers (scanners) and that Ji's invention take actions (countermeasures) on the flow if an encoded portion is determined to have a malicious code (i.e. virus) and the user is notified (i.e. an alarm is generated)

Ji fails to teach "a plurality of scanning computer systems" and distributing " copies of the flow to each of the scanning computer systems in parallel for scanning"

However, Shanklin is directed to a method of detecting unauthorized access on a network indicated by signature analysis of packet traffic on the network. A plurality of detection sensors (i.e. scanners) are connected at a network entry point associated with an internetworking device (i.e. a front- end) , see col. 1, line 61 through col. 2, line 19. Signatures detected by Shanklin's sensors include those associated with malicious intent attack (i.e. malicious codes), denial of service attack, and other method of misuse.

Shanklin teaches that the internetworking device (i.e. a front end processor) inspects packets incoming from the external network and a load balancing unit implemented in the internetworking device performs a "copy to "operation to send each packet to the sensors, see col. 6, lines 25-46, where in a detection engine examines and analyses each packet and if the analysis indicates a misuse (or a malicious code), the sensor sends an alarm to a separate detection management station to take action (i.e. countermeasure), see col. 3, lines 55-65, see also col.4, line 54 through col. 5, line 7.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ji's Gateway to include parallel sensors of Shanklin to provide a virus detection system that can keep up with the high traffic throughput of today's network, see

Shanklin's col. 2, lines 14-19, specially when Ji is also concerned in effectively detecting and eliminating viruses without significantly affecting the performance of the computer, see JI col. 2, lines 30-36. **As per claims 5 and 13**, Ji 's gateway includes FTP proxy server and a SMTP proxy server executed concurrently in a manner such that viruses transmitted to or from the network in messages and files are detected, see col. 2, lines39-67 and that the routines (i.e. scanning software) for detecting viruses (i.e. malicious codes) in the file transfers and the messages primarily include the FTP proxy server and the SMTP proxy server, see col. 4, lines 56-65. The teachings of JI clearly suggests that the gateway includes a scanning computer system configured to execute anti-virus routines having different , corresponding coverage of malicious code. That is, viruses carried by file transfers and by messages through respective FTP and SMTP proxy servers.

As per claims 6 and 14, JI teaches that the apparatus of his invention, in particular the FTP proxy server and the SMTP proxy server could be includes on a FTP server or sa world wide server for scanning files and messages as they are downloaded from the we, see col. 5, lines 28-38. This clearly suggests that Ji's invention includes the flow of Hypertext markup file and a transferred file.

As per claims 7 and 15, JI teaches that if a virus is detected, the proxy servers respond in variety of ways (i.e. a countermeasure taken) according to user's needs specified in a configuration file, see col. 11, lines 3-40, and that an action is taken based on configuration settings, such as; 1) do nothing and transfer the mail message; 2) to transfer the mail message with the encoded portions that have been determined to have viruses; 3) rename the encoded portions of the message containing viruses, store the renamed portions as files in a specified

directory (i.e. quarantining and blocking the flow) on the proxy server and notify (i.e. informing the recipient) the user of the renamed files and directory path which can be used to manually request the file from the system administrator ; 4) writing the output of virus-checking program into the mail message in place of encoded portions and sending the mail message. The teaching of JI clearly suggests a detection management system employed on the gateway connected to the proxy servers (scanners) and that Ji's invention take actions (countermeasures) on the flow if an encoded portion is determined.

Claims 2-4, 10-12, 16-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ji et al. and Shanklin et al as applied to claims 1and 9 above above, and further in view of Wells, US. Pat. No. 6,338,141, filed Sept. 1998.

As per claims 2- 4 and 10-12, JI-Shanklin fail to teach a database containing rules configured for creating a signature of a piece of malicious code detected by at least one of the scanning computer system" , " a remote site detection system" and updating the detection system by the detection manager.

However, Wells teaches method and apparatus for detecting computer viruses using a collection of relational data to detect computer viruses, see abstract. The collection of relational data comprises various relational signature objects created from viruses. That is, computer files, as they are checked for viruses , are run through a process to create those relational signature objects.

Wells's relational anti-virus engine (RAVEN) can operate from remote computer system maintaining the known virus databases, see col. 1, lines 14-20.

Wells further teaches that RAVEN may be used independently, or as part an overall anti-virus development and updating process, see col. 1, lines 46-67.

It would have been obvious to one of ordinary skill in the art to incorporate Wells's RAVEN in system of Shanklin to provide a virus detection system with high degree of certainty and to avoid false identification while recognizing new variants of known viruses, see col.2, lines 22-46.

Claim 8 is an apparatus corresponding to method claims 1-7. Claim 8 is rejected for the same reasons stated in the statement of rejections of claims 1-7 above.

Claim 16 is a method claim reciting limitations of claims 1-3, 5-7. Claim 16 is rejected for the same reasons states in the rejections of claims 1-3, 5-7 above.

Claims 17- 19 are apparatus, method and a computer –readable medium claims reciting limitations of claims 1 and 6. Claims 17-19 are rejected as such.

Claim 20 is an apparatus claim reciting limitations of claims 1 and 6. Claim 20 is rejected for the same reasons provided in the statement of rejections of claims 1 and 6 above.

Claim 21 is method claim reciting limitations of claims 1,5 and 6. Claim 21 is rejected for the same reasons provided in the statement of rejections of claims 1, 5 and 6 above.

Claims 22-23 are apparatuses implementing features of claims 1, 6 and 7. Claim 22 is rejected as such.

Claim 24 is an apparatus corresponding to method claims 1, 2 and 4. Claim 24 is rejected as such.

Claims 25-27 recite limitations of claims 1, 2, 4, 6 and 7. Claims 25-27 are rejected for the same reasons provided in the statement of rejections of claims 1,2,4,6 and 7 above.

Claims 28-30 are apparatuses implementing limitations of claims 1- 4, 6 and 7. Claims 28-29 are rejected for the same reasons provided in the statement of rejections of claims 1-4 and 6-7.

Conclusion

Any inquiry concerning this communication or earlier communications from examiner should be directed to Taghi Arani, whose telephone number is (703) 305-4274. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned is:

(703) 872-9306

Taghi Arani

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100